IN THE HIGH COURT OF JUSTICE
BUSINESS AND PROPERTY COURTS OF ENGLAND & WALES
INTELLECTUAL PROPERTY LIST (ChD)

Claim No: IL-2021-000019

B E T W E E N :

CRYPTO OPEN PATENT ALLIANCE

(for itself and as Representative Claimant on behalf of Square, Inc., Payward Ventures, Inc. (DBA Kraken), Microstrategy, Inc., and Coinbase, Inc.)

Claimant

-and-

DR CRAIG STEVEN WRIGHT

Defendant

WITNESS STATEMENT OF
ADAM BACK

I, ADAM BACK, of [redacted] will say as follows:

1. I am a cryptographer and developer in the field of cryptography. As part of my work I am the inventor of the proof-of-work system known as "Hashcash", which I described in a paper I published in 2002 under the name "*Hashcash - a denial of service counter-measure*". That is the same paper that later came to be cited in the paper known as the "Bitcoin White Paper" by Satoshi Nakamoto. Hashcash was then used as the proof of work system in Bitcoin.

2. I am also the CEO of Blockstream, a Bitcoin and blockchain technology company, although I do not make this statement in that capacity.

3. This statement has been prepared by Bird & Bird following a video interview, though I am told by Bird & Bird that our exchanges are considered privileged. This statement uses my own words and sets out facts and matters that are within my own knowledge unless otherwise stated: Where I refer to facts within my own knowledge, I believe them to be true. Where I refer to information from other sources, I have identified my sources and the information it is true to the best of my knowledge and belief.

4. On points that I understand to be important in the case, I have stated honestly (a) how well I recall matters and (b) whether my memory has been refreshed by

considering documents, and if so how and when. Although I do not know all the issues that are important to the case, I am familiar in general terms with the dispute between Craig Wright and COPA, and I am also familiar with the factual history of Craig Wright's claim to be Satoshi Nakamoto. I understand from Bird & Bird that the purpose of my evidence is to set out matters of fact and not to argue the case, and so I do not intend in this statement to address my opinion of that claim in this statement.

My correspondence with Satoshi Nakamoto

5. Bird & Bird has asked me to explain about my correspondence with Satoshi Nakamoto. On 20 August 2008, I received an email from the email address satoshi@anonymousspeech.com as follows:

> *From: satoshi@anonymousspeech.com <satoshi@anonymousspeech.com>*
> *Date: Wed, 20 Aug 2008 at 19:38*
> *Subject: Citation of your Hashcash paper*
> *To: <adam@cypherspace.org>*
>
> *I'm getting ready to release a paper that references your Hashcash paper and I wanted to make sure I have the citation right. Here's what I have:*
>
> *[5] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.*
>
> *I think you would find it interesting, since it finds a new use for hash-based proof-of-work as a way to make e-cash work. You can download a pre-release draft at http://www.upload.ae/file/6157/ecash-pdf.html Feel free to forward it to anyone else you think would be interested. I'm also nearly finished with a C++ implementation to release as open source.*
>
> *Title: Electronic Cash Without a Trusted Third Party*
>
> *Abstract: A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution. Digital signatures offer part of the solution, but the main benefits are lost if a trusted party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as honest nodes control the most CPU power on the network, they can*

> *generate the longest chain and outpace any attackers. The network itself requires minimal structure. Messages are broadcasted on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.*
>
> *satoshi@anonymousspeech.com*

6. I had not previously heard of Satoshi, but I had a few kind of academic and applied papers and I do get these sort of enquiries once in a while, so I didn't think much of it then. The pre-release draft he referred to was not attached but there was a download link to it. I believe I did download the paper at the time but didn't look at it immediately, though I did read the abstract from his email. I then went back to Satoshi on 21 August 2008 and confirmed that the citation there did seem to be right.

7. I also pointed him to another resource that I thought he would be interested in, called "B-money" by Wei Dai. He didn't seem to be aware of that, which I believe because it was not mentioned in the pre-release draft he sent me, and because he later replied on 21 August 2008 saying he was not aware of it and that he would email Wei Dai to confirm how to credit him.

8. I sent him another email later to suggest another thing he might want to look at, another paper by Revest et al called "micromint". I did not hear from Satoshi again until 10 January 2009, when he sent me an email shortly after releasing the software to say he had just released it.

9. And that was the extent of it. It was not an elaborate conversation and we didn't get into a great deal of detail. I have never published this correspondence before.

Files

{D/74}-{D/83} 10. A copy of my email correspondence with Satoshi is at Exhibit AB1. This was generated by saving them in an evidentiary way, using google mail's native export tool and adding the documents to a zip archive on my own computer, and that zip archive itself forms Exhibit AB1.

11. I don't think I have a copy of the original pre-release draft any more. At some point I did go back and look for the file but could not find it. It's possible that I might have old copies backed up somewhere, but it would have been informal and ad hoc so not likely, and I haven't been able to find one from the checks I have made.

List of documents: I have not referred to any documents other than those mentioned above.

DECLARATION OF ADAM BACK

I understand that the purpose of this witness statement is to set out matters of fact of which I have personal knowledge. I understand that it is not my function to argue the case, either generally or on particular points, or to take the court through the documents in the case. This witness statement sets out only my personal knowledge and recollection, in my own words.

On points that I understand to be important in the case, I have stated honestly (a) how well I recall matters and (b) whether my memory has been refreshed by considering documents, if so how and when.

I have not been asked or encouraged by anyone to include in this statement anything that is not my own account, to the best of my ability and recollection, of events I witnessed or matters of which I have personal knowledge. I believe the facts stated in this statement are true. I understand that proceedings for contempt of court may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief in its truth.

Signed by ADAM BACK: DocuSigned by: Adam Back C02B0BCCAF224B6... .....

Date: 17/7/2023 .....